UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/627,117	07/24/2003	Peter Dam Neilsen	857.0019.U1(US)	3924

29683 7590 12/20/2007

HARRINGTON & SMITH, PC
4 RESEARCH DRIVE
SHELTON, CT 06484-6212

EXAMINER	
TIMBLIN, ROBERT M	
ART UNIT	PAPER NUMBER
2167	

MAIL DATE	DELIVERY MODE
12/20/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/627,117	NEILSEN ET AL.	
	Examiner	Art Unit	
	Robert M. Timblin	2167	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10/4/2007*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *2,3,5-9,20,23,33,34,36-40,46 and 51-59* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *2-3, 5-9, 20, 23, 33-34, 36-40, 46 and 51-59* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

This Office Action is in regards to application 10/627,117 filed 7/24/2003).

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 10/4/2007 has been entered.

Response to Amendment

Applicant herein cancels claims 1, 4, 10-11, 13-17, 21, 25-32, 41, 44-45, 48, and 50 while adding claims 52-59. Claims 2, 3, 5, 7-9, 20, 23, 33, and 46 have been amended in this response.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 2-3, 5-9, 20, 23, 33-34, 36-40, 46 and 51-59 are rejected under 35 U.S.C. 103(a) as being unpatentable over Steele et al. ('Steele' hereinafter) (U.S. Patent Application 2002/0091700). In the following, Steel teaches and suggests

With respect to claim 2, A method as claimed 23, further comprising subsequent to step d), requesting entry of a first password to enable the further display of the first data assemblage and subsequent to step f), requesting entry of the first password to enable the further display of the second data assemblage (i.e. 0067, last 3 lines off 0120 and last 4 lines of 0123. That is, each specific file (e.g. each assemblage) may be password protected and unlocked by specification of a password).

With respect to claim 3, A method as claimed in claim 23, further comprising, before step a), wirelessly receiving the first data assemblage at the hand portable device and before step e), wirelessly receiving the second data assemblage at the hand portable device (0016; i.e. beaming of content suggests the receiving of multiple assemblages (i.e. files)).

With respect to claim 5, a method as claimed in claim 23, further comprising: discriminating the type of a data assemblage, wherein the automatic restriction of further display at step d) is enabled only for a the first data assemblage of a defined type or types (0100, top of 2nd column of page 5; e.g. the record types QAFLEAF, BITMAP LEAF, FACTONLY LEAF are associated with the characteristic flags "visited"

and "pwdProtected') and the automatic restriction of further display at step f) is enabled only for the second data assemblage of the defined type or types (0113; i.e. protecting a FACT, QAF or BITMAP page describes types of data to be protected).

With respect to claim 6, A method as claimed in claim 5, further comprising user specification of the defined type(s) for which automatic restriction of further display is enabled (0113; i.e. protecting a FACT, QAF or BITMAP page describes types of data to be protected).

With respect to claim 7 A method as claimed in claim 20, further comprising: user specification of a password for use in the first security mechanism (figure 10).

With respect to claim 8 A method as claimed in claim 23, wherein the first data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks and wherein the second data assemblage is one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks (abstract; e.g. text and graphic images).

With respect to claim 9 A method as claimed in claim 23 wherein at least one of the first data assemblage and the second data assemblage is created in the device (0120).

With respect to claim 20, Steele teaches and suggests A method comprising:

a) storing (0012) a plurality of data assemblages (Steele describes 'assemblages' as: 0014 - records, 0016 – text and image files, 0067 – leafs and records and 0103 - pages. Herein, these assemblages will be analogous to and interpreted as files) in a hand portable device (0012, 0062; i.e. PDAs and smart phones);

b) storing at least one data attribute (0077-0079; i.e. flags) for each of the plurality of data assemblages (see Steele at 0075; "flags are defined settings or triggers...associated with each record." Further, the flag definitions define the characteristics of a given record), the data attribute indicative of first display of the data assemblage in the device (see Steele at 0079; e.g. a "seen" flag describes that a leaf has been visited at least once);

c) displaying for a first time in the hand portable device (0012, 0062; i.e. PDAs and smart phones) a first data assemblage (0120; i.e. "Open Import File" describes opening a text file) of the plurality without regard to a first security mechanism (0120; i.e. it is suggested that a file may be imported without regards to a lock or entering a password), and responsive to the displaying for the first time (0079; i.e. a file is "seen") automatically changing the data attribute of the first data assemblage from a first type to a second type (0079; e.g. it is inherent that a "seen" flag would be triggered and set on if a file were to be viewed); and

d) in response to changing the data attribute (i.e. setting the "seen" flag) of step c), automatically restricting further display of the first data assemblage (0120; i.e.

locking the imaker application so that anyone opening a file after it is saved and closed will not be able to edit any password-protected page. Further, when a protected page is selected, the page is hidden (Steele at 0123) to restrict further display) using the first security mechanism (0121; i.e. password-protecting a page and requiring a password for unlocking).

Although Steel does not expressly teach automatically restricting further display, it would have been obvious to one of ordinary skill in the art at the time of the present invention to automate the locking feature to protect a specific file from being edited for the benefit password protection for a specific leaf (i.e. file). It is also suggested (in Steele's paragraph 0120) that after a file is saved and *closed* it is locked and therefore prevents further use. Also note that the flags describing the characteristics of the file (i.e. paragraphs 0077-0079) may be triggers (0075) to suggest that the flags set to protect the files can be automated.

With respect to claim 23, Stone teaches and suggests A method as claimed in claim 20, further comprising, subsequent to step d):

e) displaying for a first time in the hand portable device (0012) a second data assemblage of the plurality without regard to the first security mechanism (abstract 0102 and 0120; i.e. Steele suggests that multiple files may be navigated to and displayed), and responsive to the displaying for the first time the second data assemblage automatically changing the data attribute of a-the second data assemblage from the first type to the second type (0079; e.g. setting a "seen" flag); and

f) in response to changing the data attribute (i.e. setting the "seen" flag) of step e), automatically restricting further display of the first data assemblage (0120; i.e. locking the imaker application so that anyone opening a file after it is saved and closed will not be able to edit any password-protected page. Further, when a protected page is selected, the page is hidden (Steele at 0123) to restrict further display) using the first security mechanism (0121; i.e. password-protecting a page and requiring a password for unlocking).

With respect to claim 33, A hand-portable device, comprising:

user input means for user input of a password (figure 10);

a memory for storing data (0011);

display means for displaying the data (0019; i.e. handheld computer screen); and

access control means (col. 2 of page 5; i.e. UInt16 hidden, protected and visited) arranged to detect that the data has been displayed for a first time (0079; i.e. a "seen" flag and UInt16 visited 1 suggesting that the file has been visited (i.e. displayed) at least once (bottom of second column of page 5) at the display means (0019; i.e. handheld computer screen) and automatically responsive to detecting that the data has been displayed for the first time (0079; i.e. a file is "seen") to restrict subsequent display of the data (0120; i.e. locking the imaker application so that anyone opening a file after it is saved and closed will not be able to edit any password-protected page. Further, when a protected page is selected, the page is hidden (Steele at 0123) to restrict further display) using a first security mechanism involving the password (0121; i.e. password-

protecting a page and requiring a password for unlocking), wherein the access control means does not restrict the data being displayed for the first time using the password (0120; i.e. it is suggested that a file may be imported without regards to a lock or entering a password).

Although Steel does not expressly teach to restrict subsequent display, it would have been obvious to one of ordinary skill in the art at the time of the present invention to automate the locking feature to protect a specific file from being edited for the benefit password protection for a specific leaf (i.e. file). It is also suggested (in Steele's paragraph 0120) that after a file is saved and *closed* it is locked and therefore prevents further use. Also note that the flags describing the characteristics of the file (i.e. paragraphs 0077-0079) may be triggers (0075) to suggest that the flags set to protect the files can be automated.

With respect to claim 34, A hand-portable device as claimed in claim 33, further comprising transceiver means for wirelessly receiving the data at the hand portable device (0016; i.e. beaming of content).

With respect to claim 36, A hand-portable device as claimed in claim 33, wherein the access control means discriminates the type of data, and automatically restricts subsequent display of the data using the first security mechanism, if the data is of a

defined type or types (0113; i.e. protecting a FACT, QAF or BITMAP page describes types of data to be protected).

With respect to claim 37, A hand-portable device as claimed in claim 36, wherein the user input means is operable to enable a user to specify the defined type(s) (0075 specifying flags regarding access and protection according to a type of record).

With respect to claim 38, A hand-portable device as claimed in claim 33, wherein the user input means is operable to enable a user to specify the password (figure 10).

With respect to claim 39, A hand-portable device as claimed in claim 33, wherein the data defines one of: a SMS message, a MMS message, an instant messaging history, a picture file; an audio file; a video file; or a collection of bookmarks (abstract; e.g. text and graphic images).

With respect to claim 40, A hand-portable device as claimed in claim 33, wherein the data are created in the device (0120).

With respect to claim 46, A memory embodying a computer program and readable by a processor for enabling a mobile telephone to perform actions directed to restricting access to a first data assemblage, the actions comprising:

a) storing (0012) a plurality of data assemblages (Steele describes assemblages' as: 0014 - records, 0016 – text and image files, 0067 – leafs and records and 0103 - pages. Herein, these assemblages will be analogous to and interpreted as files) in a mobile telephone (0012, 0062; i.e. smart phone);

b) storing at least one data attribute (0077-0079; i.e. flags) for each of the plurality of data assemblages, the data attribute indicative of first display of the data assemblage (see Steele at 0075; "flags are defined settings or triggers...associated with each record." Further, the flag definitions define the characteristics of a given record), the data attribute indicative of first display of the data assemblage in the device (see Steele at 0079; e.g. a "seen" flag describes that a leaf has been visited at least once) in the mobile telephone (0012, 0062; i.e. smart phone);

c) displaying for a first time in the mobile telephone (0012, 0062; i.e. smart phone) a first data assemblage of the plurality (0120; i.e. "Open Import File" describes opening a text file) without regard to a first security mechanism, and responsive to the displaying for the first time (0079; i.e. a file is "seen") automatically changing the data attribute of the first data assemblage from a first type to a second type (0079; e.g. it is inherent that a "seen" flag would be triggered and set on if a file were to be viewed); and

d) in response to changing the data attribute (i.e. setting the "seen" flag) of step c), automatically restricting further display of the first data assemblage (0120; i.e. locking the imaker application so that anyone opening a file after it is saved and closed will not be able to edit any password-protected page. Further, when a protected page is selected, the page is hidden (Steele at 0123) to restrict further display) in the mobile

telephone using the first security mechanism (0121; i.e. password-protecting a page and requiring a password for unlocking).

Although Steel does not expressly teach automatically restricting further display, it would have been obvious to one of ordinary skill in the art at the time of the present invention to automate the locking feature to protect a specific file from being edited for the benefit password protection for a specific leaf (i.e. file). It is also suggested (in Steele's paragraph 0120) that after a file is saved and *closed* it is locked and therefore prevents further use. Also note that the flags describing the characteristics of the file (i.e. paragraphs 0077-0079) may be triggers (0075) to suggest that the flags set to protect the files can be automated.

With respect to claim 52, A hand portable device as claimed in claim 33, wherein: the data comprises a first data assemblage (0120); the memory is further for storing a second data assemblage (0012, i.e. storing image and text files), the display means is further for enabling the user to display the second data assemblage (0015; i.e. the users are allowed to rapidly navigate through large quantities of complex content), and the access control means (col. 2 of page 5; i.e. UInt16 hidden, protected and visited) is further arranged to detect that the second data assemblage has been displayed for a first time (0079; i.e. the record has been "seen") at the display means and automatically responsive to detecting that the second data assemblage has been displayed for the first time to restrict subsequent display of the second data assemblage using the first security mechanism involving the password (0075; i.e. password protection), wherein

the access control means does not restrict the second data assemblage being displayed for the first time using the first security mechanism (0120; i.e. it is suggested that a file may be imported without regards to a lock or entering a password).

With respect to claim 53, The hand portable device of claim 52, wherein at least one of the first data assemblage and the second data assemblage is created in the device (0120).

With respect to claim 54, The hand portable device of claim 33, wherein the first security mechanism comprises a data attribute associated with the data, said data attribute indicative of whether the data has been displayed for the first time (0079; "seen" flag and 0100; i.e. UInt16 visited:1 indicating that the record has been visited at least once), and wherein the access control means is arranged to restrict subsequent display of the data by changing the data attribute so as to require entry of the password at the user input means (0078; "password" flag and 0123; i.e. locking a file to prevent access to a protected page).

With respect to claim 55, The hand portable device of claim 33, wherein: the display means comprises a display (0019) and the access control means comprises a processor (0142).

With respect to claim 56, The memory of claim 46, the actions further comprising:

e) displaying for a first time in the hand portable device (0012) a second data assemblage of the plurality without regard to the first security mechanism (abstract 0102 and 0120; i.e. Steele suggests that multiple files may be navigated to and displayed), and responsive to the displaying for the first time the second data assemblage automatically changing the data attribute of a-the second data assemblage from the first type to the second type (0079; e.g. setting a "seen" flag); and

f) in response to changing the data attribute (i.e. setting the "seen" flag) of step e), automatically restricting further display of the first data assemblage (0120; i.e. locking the imaker application so that anyone opening a file after it is saved and closed will not be able to edit any password-protected page. Further, when a protected page is selected, the page is hidden (Steele at 0123) to restrict further display) using the first security mechanism (0121; i.e. password-protecting a page and requiring a password for unlocking).

With respect to claim 57, The memory of claim 56, the actions further comprising, before step a): wirelessly receiving the first data assemblage at the hand portable device and before step e), wirelessly receiving the second data assemblage at the hand portable device (0016; i.e. beaming of content suggests the receiving of multiple assemblages (i.e. files)).

With respect to claim 58, The memory of claim 56, further comprising: discriminating the type of a data assemblage, wherein the automatic restriction of

further display at step d) is enabled only for the first data assemblage of a defined type (0100, top of 2nd column of page 5; e.g. the record types QAFLEAF, BITMAP LEAF, FACTONLY LEAF are associated with the characteristic flags "visited" and "pwdProtected') or types and the automatic restriction defined type or types (0113; i.e. protecting a FACT, QAF or BITMAP page describes types of data to be protected).

With respect to claim 59, The memory of claim 46, the actions further comprising: user specification of a password for use in the first security mechanism (figure 10).

Response to Arguments

Applicant's arguments with respect to claims 20, 33, and 46 have been considered but are moot in view of the new ground(s) of rejection. Applicant's arguments, see the remarks and amendments, filed 10/4/2007, with respect to the argument pertaining to displaying for a first time without a password (i.e. security mechanism) have been fully considered and are persuasive. The 102(b) rejection of claims 20, 33, and 46 has been withdrawn. However, the newly found prior art of Steele et. al. is disclosed to teach at least this feature. Therefore Applicant's arguments are moot.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

U.S. Patent 5,644,627 to Segal et al. The subject matter disclosed therein pertains to the pending claims (i.e. detecting a read/unread condition).

U.S. Patent Application 2004/0024827 A1 to Yoshimura. The subject matter disclosed therein pertains to the pending claims (i.e. setting passwords for viewed data).

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Robert M. Timblin whose telephone number is 571-272-5627. The examiner can normally be reached on M-F 8:00-4:30.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John R. Cottingham can be reached on 571-272-7079. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should

you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Robert M. Timblin
Patent Examiner AU 2167

\

JOHN COTTINGHAM
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100